Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A server to perform computations to establish a secure network session, comprising of:

a system memory; and

a processing unit coupled to said system memory via a system bus, [[the]] said processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to [[the]] said server by [[the]] said client, [[the]] said processing unit includes:

an execution unit, coupled to a decode unit, configured to execute arithmetic instructions to perform product and square operations, [[the]] said execution unit including ~~at least one adder and~~ at least two multipliers connected directly with said system memory for multiplying data provided from said system memory, and at least one adder connected directly with said at least two multipliers for applying an addition operation to outputs of said at least two multipliers, said execution unit configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel;

[[the]] said decode unit to receive requests for establishing a secure network session from [[the]] said client, [[the]] said decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, [[the]] said decode unit further configured to issue [[the]] said arithmetic instructions to [[the]] said

execution unit so that [[the]] said execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either [[the]] said square or product operation.

2. (Currently Amended) The server of claim 1, wherein [[the]] said decode unit is configured to issue a set of instructions that causes [[the]] said execution unit to perform [[the]] said specified multiplication and addition operations in parallel to ~~reduce the~~ reduce a number of cycles required to perform [[the]] said product operation.

3. (Cancelled)

4. (Currently Amended) The server of claim 3, wherein certain of [[the]] said multiplication operations are performed in parallel using a multiply and shift by one instruction.

5 - 6. (Cancelled)

7. (Currently Amended) The server of claim 1, wherein [[the]] said decode unit is further configured to decode an operation $M=C^d \bmod N$ by:

(a) determining ~~the MSB~~ a MSB position of ~~the exponent~~ an exponent d equal to a first logic state;

(b) issuing a first set of instructions to implement a square and a product operation after [[the]] said MSB position of [[the]] said exponent d equal to ~~a first~~ the first logic state is determined;

(c) determining if ~~the next~~ a next most significant bit (MSB) of ~~exponent (d)~~ said exponent d is of the first logic state or a second logic state; and either

(d) issuing a second set of instructions to [[the]] said execution unit to implement a square operation if [[the]] said next MSB is of [[the]] said second logic state; or

(e) issuing [[the]] said first set of instructions to [[the]] said execution unit if [[the]] said next MSB ~~of the exponent~~ said exponent d is of [[the]] said first logic state to implement a square and a product operation; and

repeating (c) through (e) for every bit in the ~~exponent (d)~~ said exponent d from [[the]] said next MSB to ~~the least~~ a least significant bit (LSB).

8. (Currently Amended) The server of claim 7, wherein ~~the final~~ a final result of [[the]] said operation $M=C^d \bmod N$ is obtained by accumulating ~~the results~~ results of (b) through (e).

9. (Currently Amended) The server of claim 1, wherein [[the]] said encryption processor is located in [[the]] said server and is used to establish a secure socket layer connection between [[the]] said server and [[the]] said client.

10 - 11. (Cancelled)

12. (Currently Amended) The server of claim 1 wherein [[the]] said product and square operations executed by [[the]] said execution unit are Montgomery product and square operations.

13. (Cancelled)

14. (Currently Amended) The server of claim 1, wherein [[the]] said encryption processor is configured into a web server deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

15. (Currently Amended) The server of claim 1, wherein [[the]] said encryption processor is configured into a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

16. (Currently Amended) The server of claim 1, wherein [[the]] said encryption processor is configured into an Internet load balance device with Secure Socket Layer (SSL)/Transport Layer Security(TLS) termination functionality.

17. (Currently Amended) The server of claim 1 wherein [[the]] said encryption processor is configured into an Internet appliance for a Virtual Private Network.

18. (Currently Amended) The server of claim 1 wherein [[the]] said encryption processor is configured into a security based router.

19. (Currently Amended) The server of claim 1 wherein [[the]] said encryption processor is configured into a remote access device used for VPN applications.

20. (Currently Amended) The server of claim 1, wherein [[the]] said encryption processor is configured into one or more of the following: concentrator-based security systems for enterprise and ISPs; subscriber management systems with VPN support; firewalls with VPN support; and VPN gateways.

21. (Currently Amended) A method to establish a secure network session, comprising the steps of:

sending an encrypted message to a server using a public key;

decrypting said encrypted message by [[the]] said server using a private key; and

generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and [[the]] said server, wherein generation of [[the]] said public key, [[the]] said private key, and/or [[the]] said symmetrical key further comprises computation of a modular exponentiation operation ~~using the~~ using a Montgomery method, wherein said Montgomery method further comprises:

receiving, by a decode unit, a request to perform a modular operation;

determining, by [[the]] said decode unit, whether a Montgomery square operation or a Montgomery product operation is to be performed;

issuing, by [[the]] said decode unit, a first instruction to perform a Montgomery square operation;

issuing, by [[the]] said decode unit, a second instruction to perform a Montgomery product operation;

performing, by an execution unit, simultaneous multiplication operations in response to at least one of [[the]] said first instruction and [[the]] said second instruction; and

performing, by [[the]] said execution unit, simultaneous multiplication and addition operations in response to at least one of [[the]] said first instruction and [[the]] said second instruction.

22. (Currently Amended) A method to establish a secure network session, comprising the steps of:

sending an encrypted message to a server using a public key;

decrypting said encrypted message by said server using a private key; and

generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and said server, wherein said public key, said private key, and/or said symmetrical key further comprises computation of a modular exponentiation operation ~~using the~~ using a Montgomery method, wherein said Montgomery method further comprises:

determining, by a decode unit, whether to perform a Montgomery square operation or a Montgomery product operation;

issuing, by [[the]] said decode unit, a first set of instructions for an execution unit to perform [[the]] said Montgomery square operation, [[the]] said first set of instructions ~~comprising;~~ comprising:

a first instruction to perform simultaneous multiplication operations; and

a second instruction to perform simultaneous multiplication and addition operations; and

issuing, by [[the]] said decode unit, a second set of instructions for [[the]] said execution unit to perform [[the]] said Montgomery product operation, [[the]] said second set of instructions comprising:

a third instruction to perform simultaneous multiplication operations;

a fourth instruction to perform simultaneous multiplication and addition operations; and

a fifth instruction to perform simultaneous multiplication and addition operations.

23. (Currently Amended) The server of claim 1, wherein ~~the at least one adder and at least two multipliers~~ said at least two multipliers and said at least one adder perform [[the]] said specified multiplication operations in parallel in a first clock cycle.

24. (Currently Amended) The server of claim 23, wherein ~~the at least one adder and at least two multipliers~~ said at least two multipliers and said at least one adder perform [[the]] said specified multiplication and addition operations in parallel in a second clock cycle that immediately follows [[the]] said first clock cycle.

25. (Currently Amended) The server of claim 1, wherein ~~the at least one adder and at least two multipliers~~ said at least two multipliers and said at least one adder perform either specified multiplication operations in parallel or perform specified multiplication

and addition operations in parallel in accordance with [[the]] said arithmetic ~~issued~~ instructions.

26. (Currently Amended) The server of claim 1, wherein [[the]] said decode unit determines whether a square operation or a product operation needs to be performed on an operand for a modular operation.

27. (Currently Amended) The server of claim 26, wherein ~~the at least one adder and at least two multipliers~~ said at least two multipliers and said at least one adder perform either specified multiplication operations in parallel or perform specified multiplication and addition operations in parallel in accordance with the determination of whether a square operation or a product operation needs to be performed.

28. (Currently Amended) The server of claim 1, wherein [[the]] said arithmetic instructions comprise a set of micro instructions.

29. (Currently Amended) The server of claim 1, wherein [[the]] said arithmetic instructions comprise plurality of types of add-subtract instructions and a plurality of types of multiply instructions.

30. (Currently Amended) The server of claim 1, wherein [[the]] said value for clear text M is calculated using [[the]] said Montgomery method.